

VANET: Analysis of Black hole Attack using CBR/UDP Traffic Pattern with Hash Function and GPSR Routing Protocol

PoojaDahiya¹, Radhika², Dr. Pankaj Gupta³, Dr. Deepak Goyal⁴, Monika Goyal⁵

¹Student - Vaish College Of Engineering , Department of Computer Science and Engineering
Rohtak, Haryana, India

²Assistant Professor - Vaish College Of Engineering , Department of Computer Science and Engineering,
Rohtak, Haryana, India

³Professor - Vaish College Of Engineering , Department of Computer Science and Engineering,
Rohtak, Haryana, India

⁴Associate Professor - Vaish College Of Engineering , Department of Computer Science and Engineering,
Rohtak, Haryana, India

⁵Lecturer– Vaish Mahila Mahavidyalaya, Rohtak (Haryana), India

Abstract –With momentum of time huge development occurred in the field of MANET and VANET. As we know when new technology emerges it came with many advantages but definitely some limitation must be there. In WSN security is one of biggest challenges which we need to tackle to implement adhoc network. Main reason behind this is dynamic topology of sensing node because nodes are dynamic in nature rather than static. As technology came into existence side by side unethical activity also take place which try to access the data illegally to gain personnel profit. There are so many types of attack possibilities are there in adhoc network. Attack can be classified into active and passive. In our research article our main concern is on black hole attack. According to this attack a malicious node with high priority number is deployed in between other nodes. Now this malicious node access the data and sends acknowledgement to source that data received. Source node will think that acknowledgement is sent by destination node but actually it is sent by malicious node. In this research article performance analysis of the black hole attack in Vehicular Ad Hoc Network is executed. The networking parameters are considered to analyze the impact of black hole attack and networking parameters are end to end delay, packet loss, energy consumption. In this paper implementation of black hole attack, secure black hole attack and GPSR protocol executed and a comparative analysis of these executed successfully and result are simulated in NS 2 which are depicted in simulation result section of article. Security algorithm play very crucial role so that unauthorized person cannot access the original information.

Index Terms –Black Hole Attack, Network, Secure, End to End Delay, Adhoc, Protocol, VANET, Packet

1. INTRODUCTION

Underwater VANET is a booming technology that has attracted several organizations. Security parameters in VANET are now receiving popularity in the research community. In VANET environment, significant decision format has to be determined with the problems related to attack modeling, optimizing response and allotment of defense resources in a wide manner. However, a single defense mechanism cannot provide solution to the attack models that are affecting the VANETs. The game theory model is used as a defense mechanism against sophisticated and complex type of attacks arising in VANET.

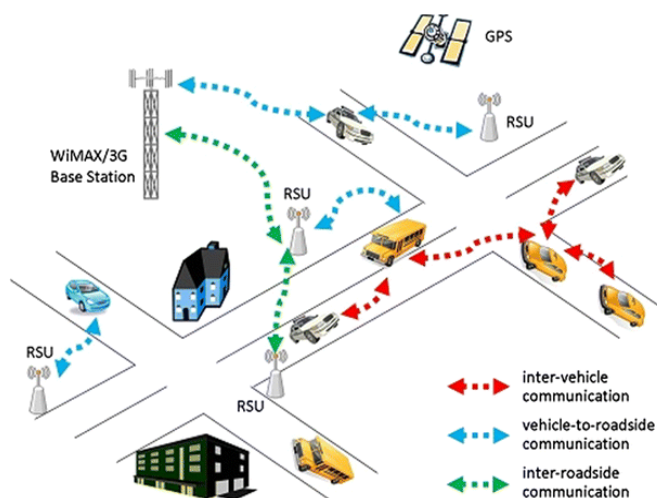


Figure1 Configuration of Vehicular Ad hoc Networks

Securing wireless adhoc networks is a highly challenging issue. Understanding possible form of attacks is always the

first step towards developing good security solutions. Security of communication in MANET is important for secure transmission of information [4]. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET. These attacks can be classified into two types:

Passive Attacks: Passive attacks are the attack that does not disrupt proper operation of network .Attackers snoop data exchanged in network without altering it. Requirement of confidentiality can be violated if an attacker is also able to interpret data gathered through snooping .Detection of these attack is difficult since the operation of network itself does not get affected [7-8].

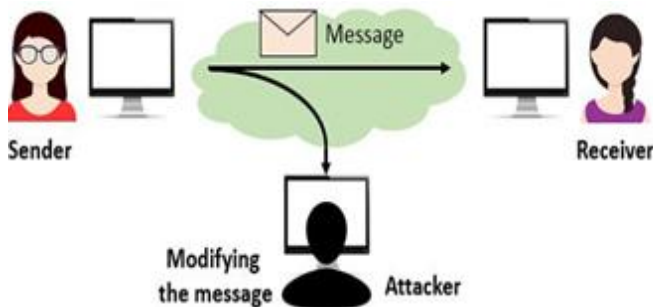


Figure2 Passive Attack

Active Attacks: Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the attacks. Active attacks involve some modification of data stream or creation of false stream. Active attacks can be internal or external.

- External attacks are carried out by nodes that do not belong to the network.
- Internal attacks are from compromised nodes that are part of the network.

Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation (masquerading or spoofing), modification, fabrication and replication

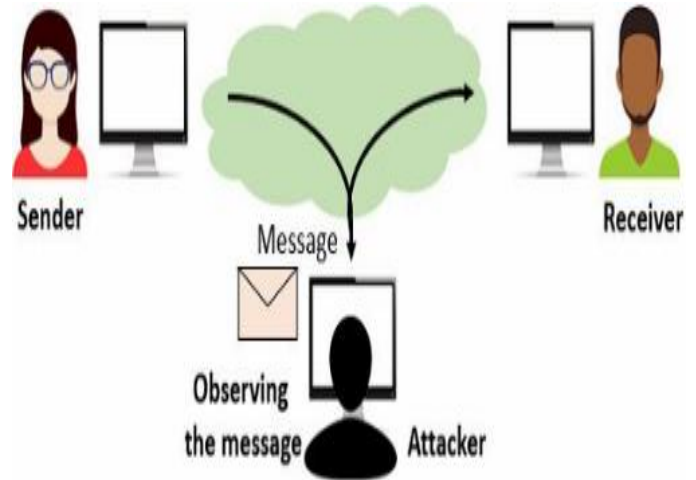


Figure 3 Active Attack

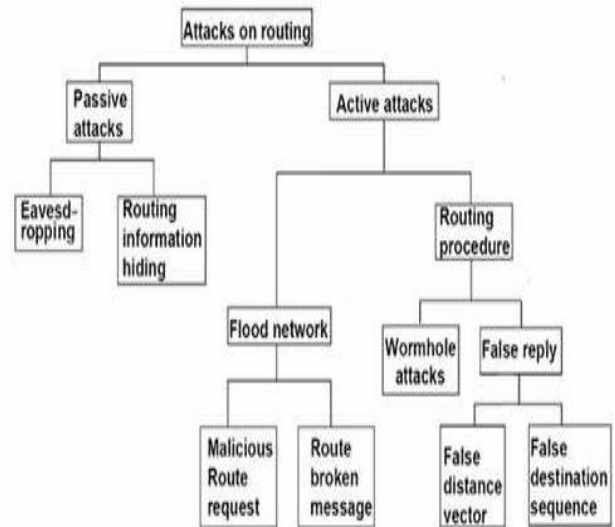


Figure 4 Classifications of Attacks in WSN

Black hole Attack: In this attack, an attacker advertises a zero metric for all destinations causing all nodes around it to route packets towards it. A malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. A malicious node drops all packets that it receives instead of normally forwarding those packets. An attacker listen the requests in a flooding based protocol [11-13].

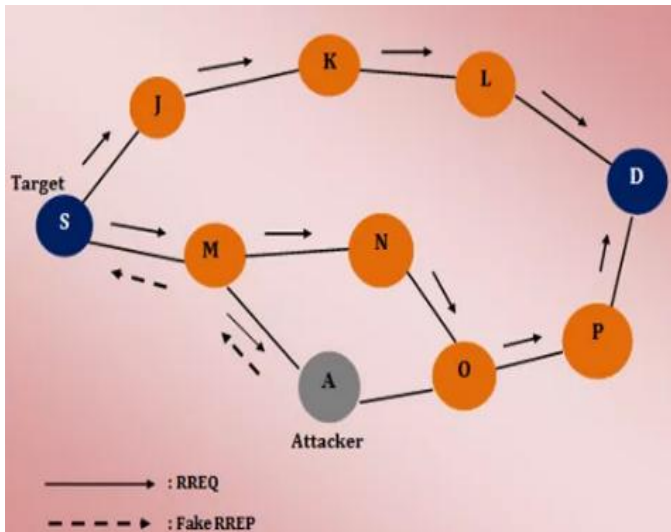


Figure 5 Scenario of Black hole attack in Networks

2. RELATED WORK

AODV routing is an extensively accepted routing protocol for MANET. The inadequacy of security considerations in the design of AODV makes it vulnerable to black hole attack. In a black hole attack, malicious nodes attract data packets and drop them instead of forwarding. Among the existing black hole detection schemes, just a few strategies manage both single and collaborative attacks and that too with much routing, storage and computational overhead. This paper describes a novel strategy to reduce single and collaborative black hole attacks, with reduced routing, storage and computational overhead. The method incorporates fake route request, destination sequence number and next hop information to alleviate the limitations of existing schemes [6]. VANETs are becoming popular and promising technologies in the modern intelligent transportation world. They are used to provide an efficient Traffic Information System, Intelligent Transportation System and life Safety. The mobility of the nodes and the volatile nature of the connections in the network have made VANET vulnerable to many security threats. Black hole attack is one of the security threat in which node presents itself in such a way to the other nodes that it has the shortest and the freshest path to the destination. Hence in this research paper an efficient approach for the detection and removal of the Black hole attack in the VANET is described. The proposed solution is implemented on AODV routing protocol one of the most popular routing protocol for VANET. The simulation is carried on NS2 and the results of the proposed scheme are compared and the fundamental AODV routing protocol, this results are examined on various network performance metrics such as packet delivery ratio, throughput and end-to-end delay. The found results show the efficacy of the proposed method as throughput and the delivery ratio of the network does not deteriorate in presence of the back holes [1]. VANET are the

promising approach to provide safety to the drivers and which is a growing technology. VANET is the new form of MANET. There are different types of attack but in our paper we are discussing about Black hole attack. There are two types of traffic pattern CBR and TCP. In this paper, we are analyzing the Black hole attack using CBR (Constant Bit Rate) and TCP traffic pattern in Manhattan Grid scenario under AODV protocol. The purpose of this paper is to analyzing the different traffic pattern with Black hole attack and without Black hole attack on the basis of Performance metrics [2]. Utilization of mobile devices is burgeoning rapidly and consequently mobile ad-hoc networks (MANETs). The self configuring and infrastructure less property of MANETs makes them easily deployable anywhere and extremely dynamic in nature. lack of centralized administration and coordinator are the reasons for MANET to be vulnerable to active attack like black hole. Black hole attack is ubiquitous in mobile ad hoc as well as wireless sensor networks. Black hole affected node, without knowing actual route to destination, spuriously replies to have shortest route to destination and entice the traffic towards itself to drop it. Network containing such node may not work according to the protocol being used for routing. Commonly used protocols like ADOV, DSR, and so forth in MANET are not designed to tackle black hole attack or black hole affected routes. Hence this paper proposes an AODV-based secure routing mechanism to detect and eliminate black hole attack and affected routes in the early phase of route discovery. A validity value is attached with RREP which ensures that there is no attack along the path. The proposed method is simulated in NS2 and performance analysis is carried out [3]. Routing in vehicular ad-hoc network is current area of research due to fast mobility of vehicles. A new route in very less time has to be developed to communicate with the base station. If any node behaving like malicious and creates attack on network, than whole communication will be squeeze. This paper presents a routing strategy to prevent from attack and identify the malicious node. The strategy has been implemented on QualNet 5.0 and compared with other routing protocols in the presence of malicious nodes [5].

3. METHODOLOGY

Objective: The main task of this research is to simulate the performance result of the proposed routing protocol with mobility model. Objective of research divided as and depicted below:

1. Firstly, simulation environment is to be setup NS-2.35
2. To Analysis the performance of base and proposed routing protocol in VANET.
3. To Compare the Results under these parameters given as Throughput, Packet Delivery Ratio, E2E delay, Over-Head and Energy.

4. Reporting and analysis of the results obtained in graphical form.

Algorithm

With the assistance of node in ns-2.35 generate a road topology. Every vehicle keeps a neighbouring database based on their current location after regular interval of time. Information data are transfer to next-hop neighbour. If a Vehicle does not receive messages from hop neighbour during a certain time duration, after then the link is lost and for route estimation a graph $G(V, E)$ theory is used to consisting of a road inter-section point or topographic point $j \in I$ and road segments $c \in C$ here every portion are attached with the inter-section point.

```

** The sender sends a RREQ packet which contains a plain text.
When a node recieved the RREQ packet
if(not(Reciever)) then
if((has optimum route path to recieved) ||
(has shorter route to reciever) then
Save the reverse route & Forward the packet
if
else
Encrypt the plaintext in the packet with
    Hash function
Send a RREP towards the sender with the cipher text
if
When a node nodes recieved a RREP data
If(not(Sender)) then // By Sender we mean the
// original source of the RREQ packet
After then Forward the packet towards sender
else
if(RREP packet contains the required cipher) then
Forward data packets to the last forwarder
of the RREP packet
else
Drop the RREP packet

```

Figure 6 Steps involving for sending packets

4. SIMULATION RESULT

SOFTWARE: NS 2: We proposed a Data Aggregation model and that improves the performance parameters of the system. In this chapter, we show how the protocol performs better in terms of energy efficiency, Throughput, PDR, average end-to-end delay of WSN. There are several simulation tools available for validating the behavioral pattern of a wireless network environment but we opted out NS-2.35 as our tool in simulating the proposed protocol.

Table 1: Simulation parameters in NS2

PARAMETERS	VALUES
Operating System	Linux (Ubuntu 12.04)
NS-2 version	NS-2.35 for IEEE 802.11Ext
No. of vehicles	10, 20, 30, 40,50
Number of Road Segments	4
Speed of vehicles	20 m/sec.
Radio propagation model	Propagation/Two Ray Ground
Network interface type	Phy /Wireless PhyExts
Packet Size	512
Traffic Type	UDP-CBR
Execution Time	100sec
Antenna Type	Omni-Antenna
Transmission Range	1000*1000 m
Routing Protocol (Proposed)	AODV,GPSR, CA, Hash function
Rx power	0.3
Tx power	0.6
Initial Energy	90
Interface Queue Length	200
Mobility Model	Manhattan Mobility Model

Optimal Route Selection

Procedure 1: route discovery

Input: ID of source node S and Destination node E

Outputs: optimal route from source to destination

Begin

If (ID E = ID N)

Forward packet to E;

Else

Determine the rectangle restricted searching area;

searching_area = [Xmin, Xmax, Xmin, Xmax];

Broadcast RREQ to E in the searching_area;

Activate (BROADCAST_TIMER);

Calculate route discovery, connectivity and packet dropping;

if (p max - p other > F)

return route with the discovery of connectivity pmax;

else

delete routes with the discovery of connectivity p other < pmax - p threshold;

return route with packet delay d min;

end if

end if

End of Route Discovery

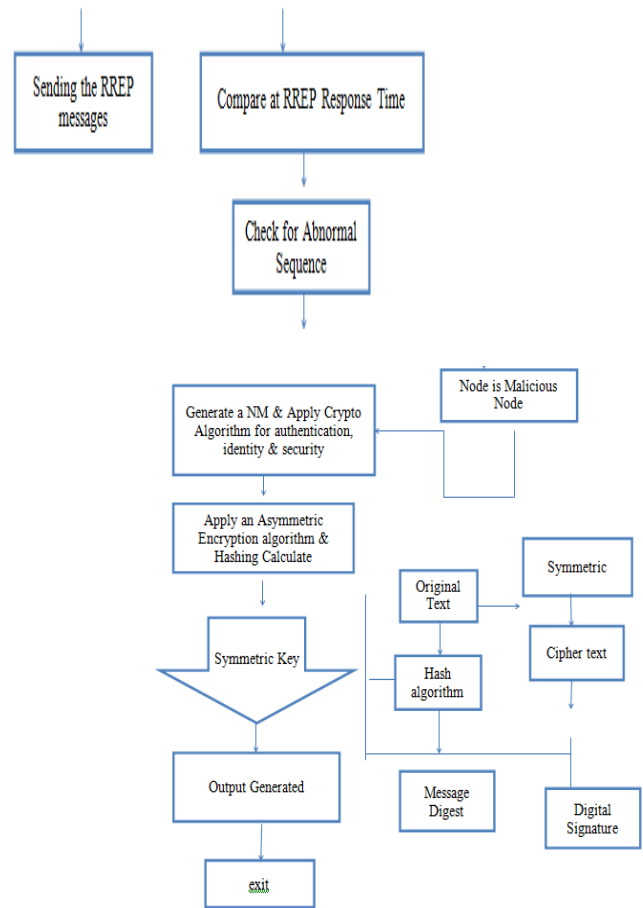
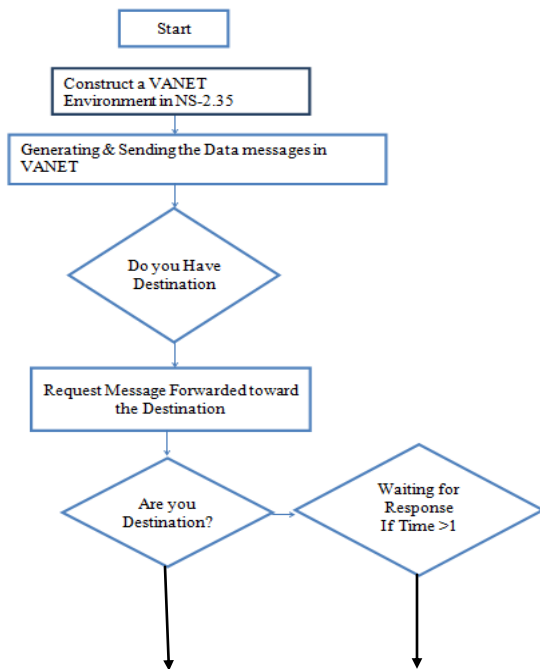


Figure 7 Methodology's Flowchart

Flowcharts for Methodology



End-to-End Delay

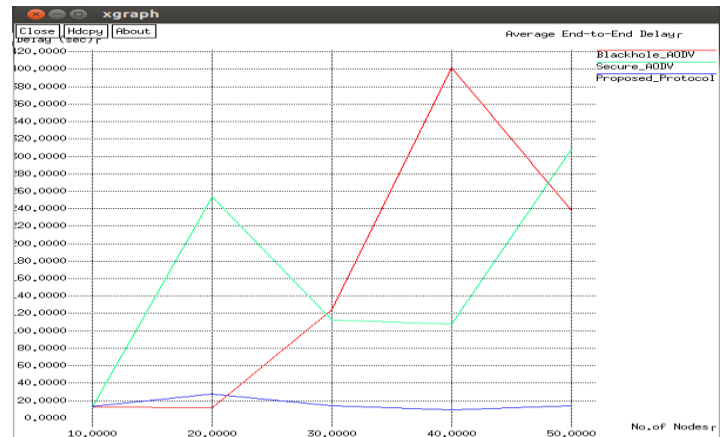


Figure 8 Comparison of average end-to-end delay

Energy Consumption

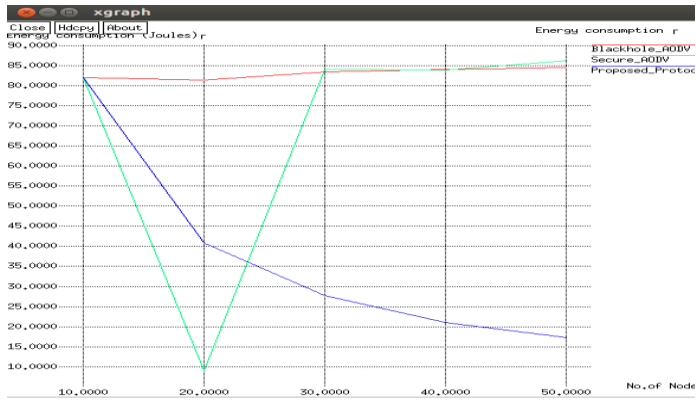


Figure 9 Comparison of Energy Consumption

Overhead

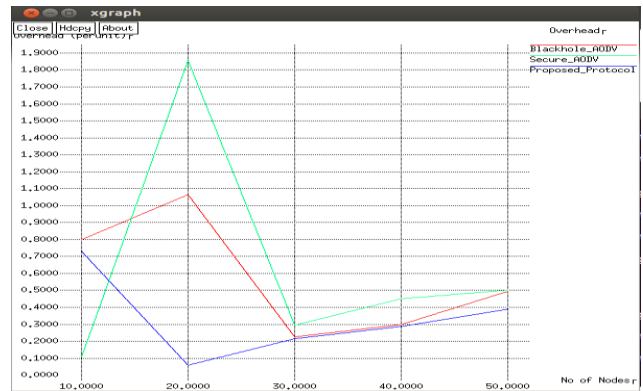


Figure 12 Comparison of Overhead

Packet Delivery Ratio

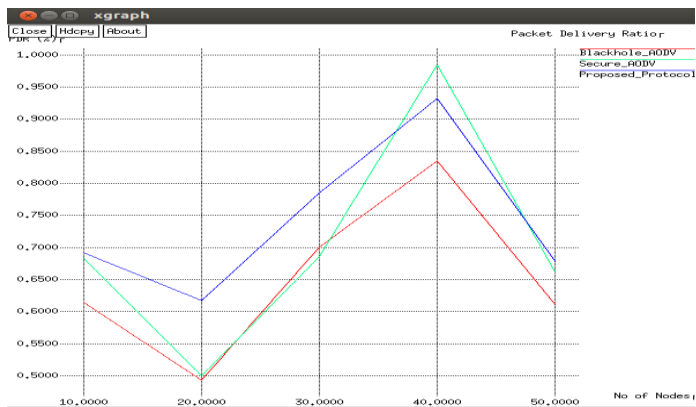


Figure 10 Comparison of Packet Delivery Ratio

Malicious Node Simulation Result for 50 Nodes

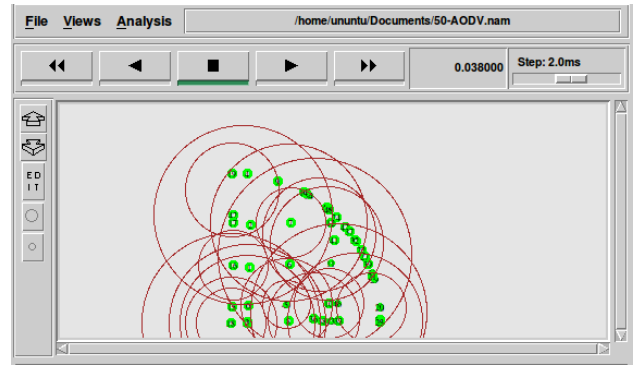


Figure 13 Initial stages for nodes showing their respective position

Throughput

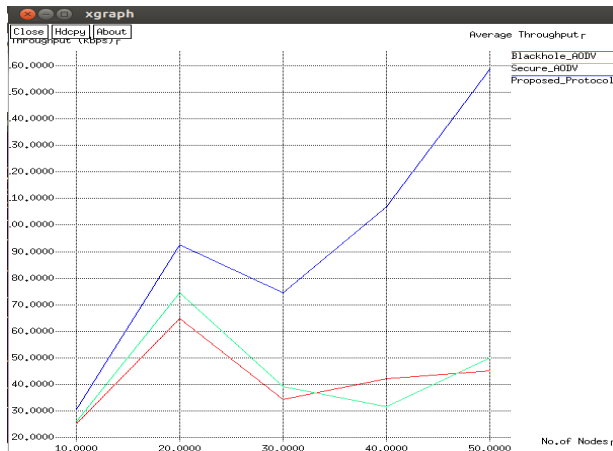


Figure 11 Comparison of Throughput

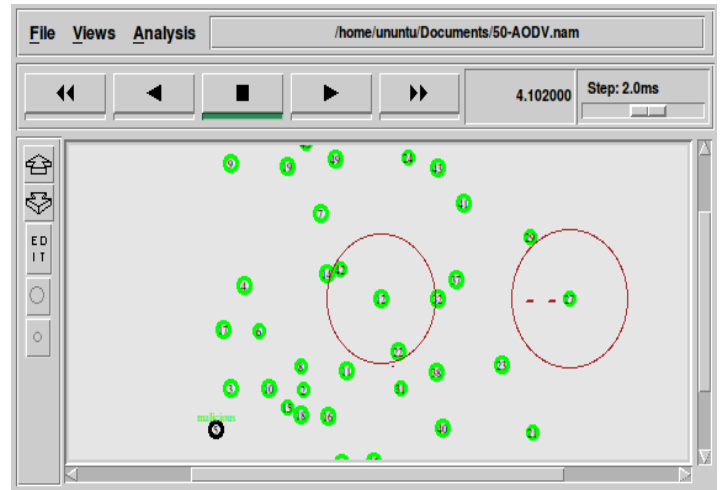


Figure 14 Trans mission between node 12 and 27, Node 5 is malicious node

AODV Protocol Simulation Result for 50 Nodes

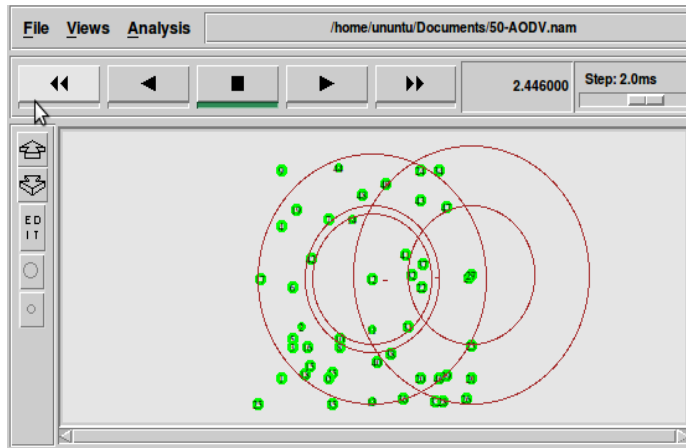


Figure 15 Cluster formed and data transmission between node 27 and 12

5. CONCLUSION

VANET is a part of MANET and it is specific application oriented. This network can be established at nadir situation where a conventional network cannot be deployed. Deploying VANET there are technical and social challenges. Concern of security in implementing of VANET is crucial parameter. In our base work black hole attack used in network communication using AODV protocol. In NS 2 environment implementation of black hole attack, secure black hole attack and GPSR protocol executed and a comparative analysis of these executed successfully. As technology came into existence side by side unethical activity also take place which try to access the data illegally to gain personnel profit. Few times back almost a decade must require in inventing new technology but in recent time after every 4 to 5 year new technology hit the market. Further this work can be extended in better way with help of internet of thing (IoT), M2M (machine to learning) and artificial intelligence (AI).

6. FUTURESCOPE

A further research has to be done in the cluster procedure especially in the initial phase where the cluster groups are formed. For an efficient clustering algorithm the time taken to complete the formation of the cluster team is very crucial. Delay in the initial phase of clustering means more packet transmissions and more power consumption. An important subject that also needs further investigation is the effect of adding more sensor nodes into the network system after the initial clustering phase. Furthermore, the re-clustering process

that can give a solution to the previous issues requires further, in depth with security.

7. REFERENCES

- [1] Salim Lachdhaf, Mohamed Mazouzi, "Detection and Prevention of Black Hole Attack in VANET Using Secured AODV Routing Protocol", Conference Paper, DOI: 10.5121/csit.2017.71503 Natarajan Meghanathan et al. (Eds) : NeT CoM, CSEIT, GRAPH-HOC, NCS, SIPR – 2017 pp. 25– 36, 2017
- [2] Bharti, D.P. Dvedi, "Performance Analysis of Black hole Attack using CBR/UDP Traffic Pattern with AODV routing Protocol in VANET", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2016): 6.391
- [3] Sagar R Deshmukh, P N Chatur, Nikhil B Bhople, "AODV-Based Secure Routing Against Black hole Attack in MANET", IEEE International Conference On Recent Trends in Electronics Information Communication Technology, India, pp. 1960-1964, 2016
- [4] Heithem Nacer and Mohamed Mazouzi, "A Scheduling Algorithm for Beacon Message in Vehicular Ad Hoc Networks", International Conference on Hybrid Intelligent Systems (HIS 2016), Marrakech, Morocco, pp. 489-497, 2016.
- [5] Roshan Jahan, Preetam Suman, "Detection of malicious node and development of routing strategy in VANET", 3rd International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, pp. 472-476, 2016
- [6] Sathish M, Arumugam K, S. Neelavathy Pari, Harikrishnan V S, "Detection of Single and Collaborative Black Hole Attack in MANET", International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), IEEE, pp. 2040-2044, 2016.
- [7] Sathish M, Arumugam K, S. Neelavathy Pari, Harikrishnan V S, "Detection of Intelligent Malicious and Selfish Nodes in VANET using Threshold Adaptive Control", 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA), IEEE, 2016
- [8] P.S Hiremath and Anuradha T, "Adaptive Fuzzy Inference System for Detection and Prevention of Cooperative Black Hole Attack in MANETs", International Conference on Information Science (ICIS), pp. 245-251, 2016
- [9] P.S Hiremath and Anuradha T, "Adaptive Method for Detection and Prevention of Cooperative Black Hole Attack in MANETs", International Journal of Electrical and Electronics and Data Communication, Volume-3, Issue-4, pp. 1-7, 2015
- [10] R. Khatoun, P. Guy, R. Doulati, L. Khoukhi and A. Serhrouchni, "A Reputation System for Detection of Black Hole Attack in Vehicular Networking", International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC), 2015
- [11] Surmukh, S.; Kumari, P.; Agrawal, S. Comparative Analysis of Various Routing Protocols in VANET. In Proceedings of 5th IEEE International Conference on Advanced Computing & Communication Technologies, Haryana, India, 21–22 February 2015
- [12] Elias C. Eze, Sijing Zhang and Enjie Liu, "Vehicular Ad Hoc Networks (VANETs): Current State, Challenges, Potentials and Way Forward", Proceedings of the 20th International Conference on Automation & Computing, Cranfield University, Bedfordshire, UK, 2014
- [13] Sabihur Rehman, M. Arif Khan, Tanveer A. Zia, Lihong Zheng, "Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges", Journal of Wireless Networking and Communications, 2013, pp. 29-38.
- [14] Sirwan A. Mohammed and Sattar B. Sadkhan, "Design Of Wireless Network Based On Ns2", Journal of Global Research in Computer Science (jgrcs), Volume 3, No. 12, December 2012.

[15] HalabiHasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan,” Denial of Service (DOS) Attack and Its Possible Solutions in VANET”, Intemational Scholarly and Scientific Research & Innovation 4(5) 2010, World Academy of Science, Engineering and Technology, Vol:4 2010-05-25.